CHECK POINT™

YOU DESERVE THE BEST SECURITY

PERFORMANCE OPTIMIZATION PART 2 - SECUREXL

We will start soon!

Valeri (VAL) Loukine

Cyber Security Evangelist | Community Lead

CheckMates Live Virtual Series 2022

Check Point CHECKMATES

CHECK POINT™

YOU DESERVE THE BEST SECURITY

PERFORMANCE OPTIMIZATION

Part 2 - **SecureXL**

PhoneBoy

Cyber Security Evangelist | Community Lead

CheckMates Live Virtual Series 2023

Check Point CHECKMATES

Housekeeping Rules

- The session is being recorded, all participants will get a link
- Materials will be posted on CheckMates
- Use Q&A panel for questions, not Chat
- You can up-vote there questions from others
- Raising a hand is an option
- Speak your mind

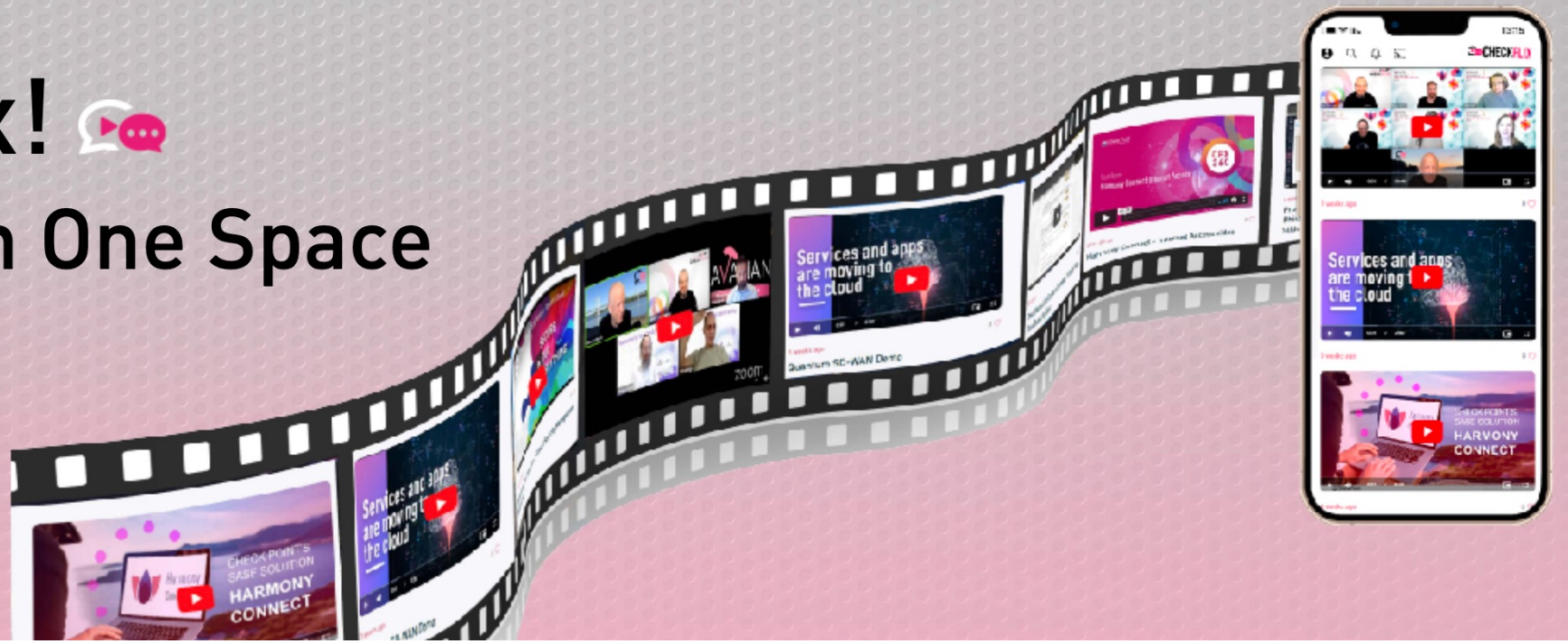
Check Point
CHECKMATES

Check Point
CHECKMATES

CheckFlix!

All Videos In One Space

WATCH NOW



CHECKMATES TOOLBOX

CHECKMATES LAB

TECH TALKS

CP <DEV>

CheckMates LIVE

CHECKMATESGO

Check Point CLOUDMATES

C P·4·B
CHECK POINT FOR BEGINNERS

CHECKFLIX

Check Point
CHECKMATES
Partner Community

community.checkpoint.com

Full list of Performance Series

- Part 1 – Introduction
- **Part 2 – SecureXL**
- Part 3 – CoreXL
- Part 4 – Clustering and Hyperscale
- Special– Diagnostics How To

Agenda

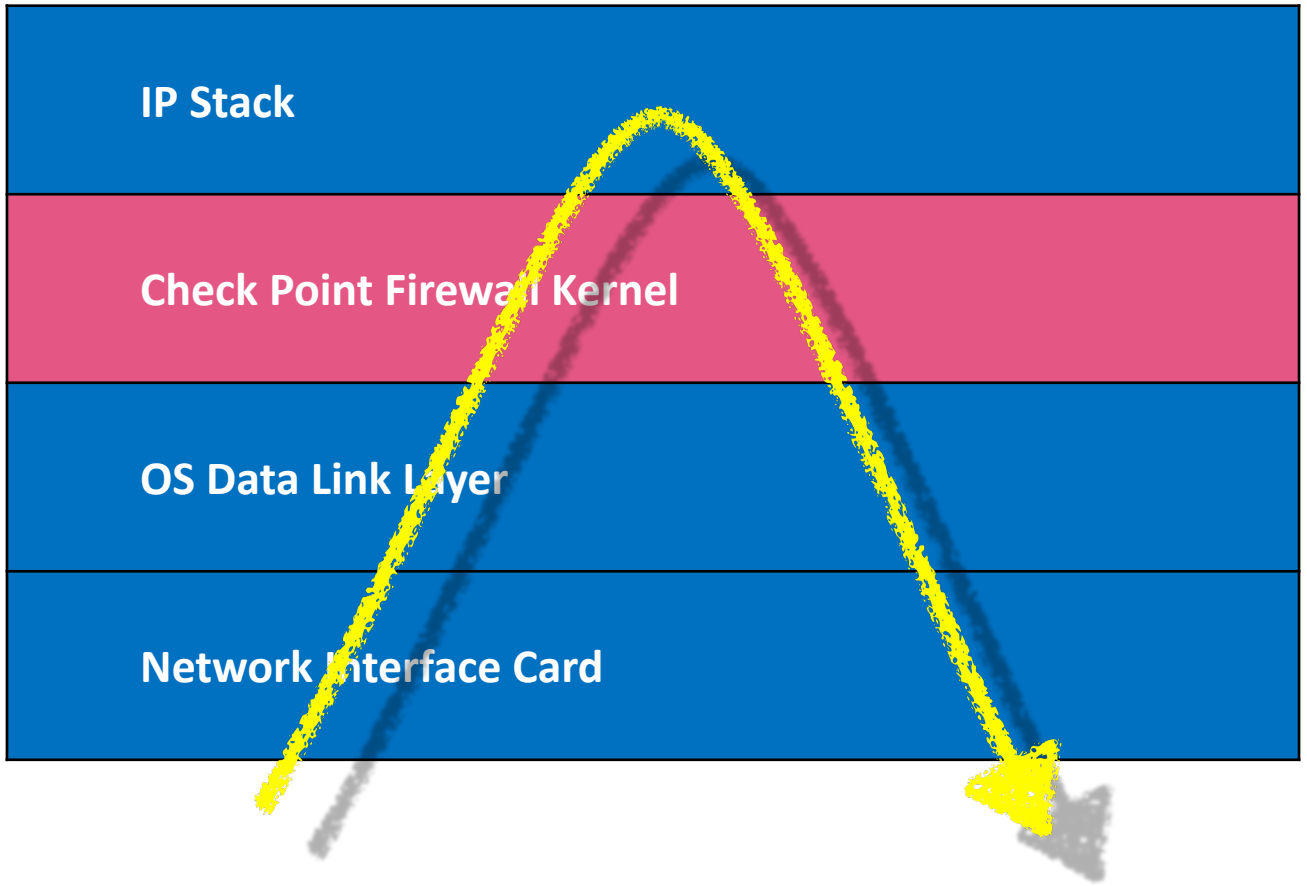
- Quick re-cap
- SecureXL in depth
  - Terminology
  - Architecture
  - Optimization
  - Tools

Performance of Security Gateway depends on

- CPU - utilization / saturation / errors
- Memory - utilization / saturation / errors
- Network Interfaces - utilization / saturation / errors
- Storage device I/O, capacity, controller - utilization / saturation / errors
- Throughput (packet rate * packet size)

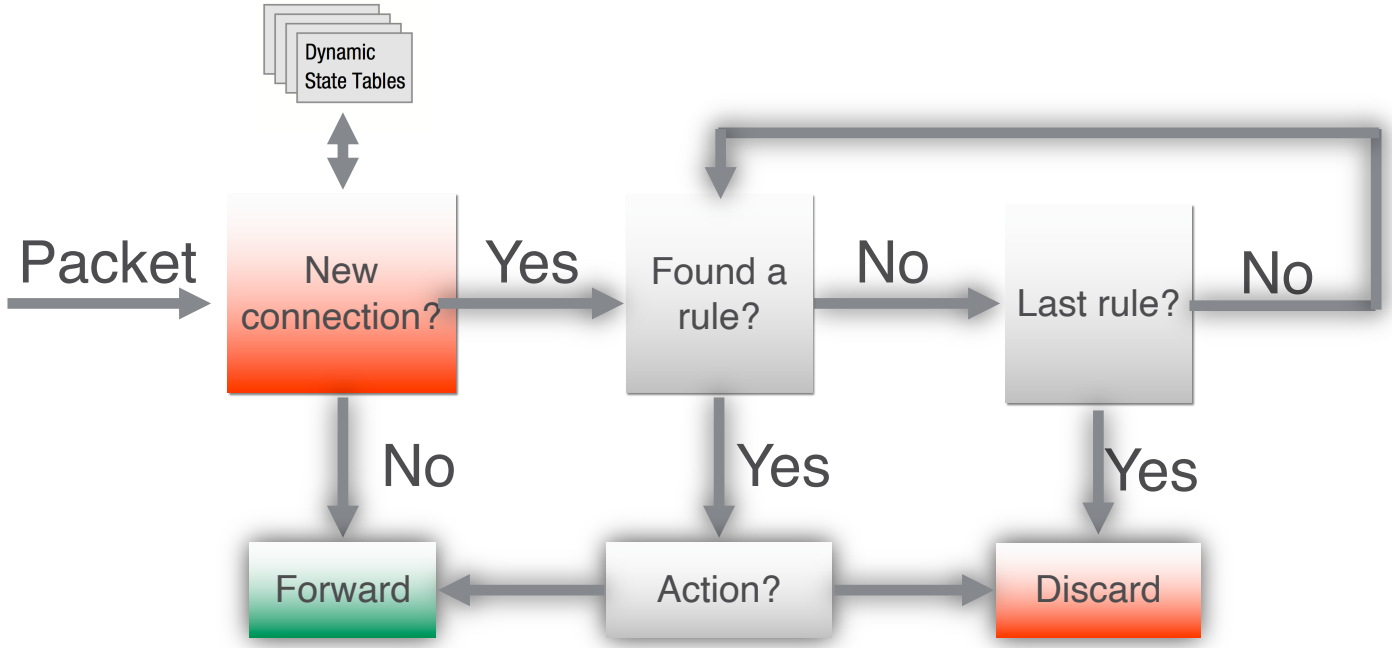
sk98348

Stateful Inspection



Stateful Inspection

- The best network security idea in the last 30 years
- Come with an eventual performance drag



Stateful Inspection as a performance bottleneck

- Confined in kernel space (originally)
- Cannot pass through before inspection
- Matching first packet takes lots of effort
- Dropping takes even more effort

Network Performance Terminology

- Throughput
- Packet per second rate
- Latency
- Number of concurrent connections
- New connection rate
- Jitter and Retransmissions

SECUREXL

Why SecureXL?

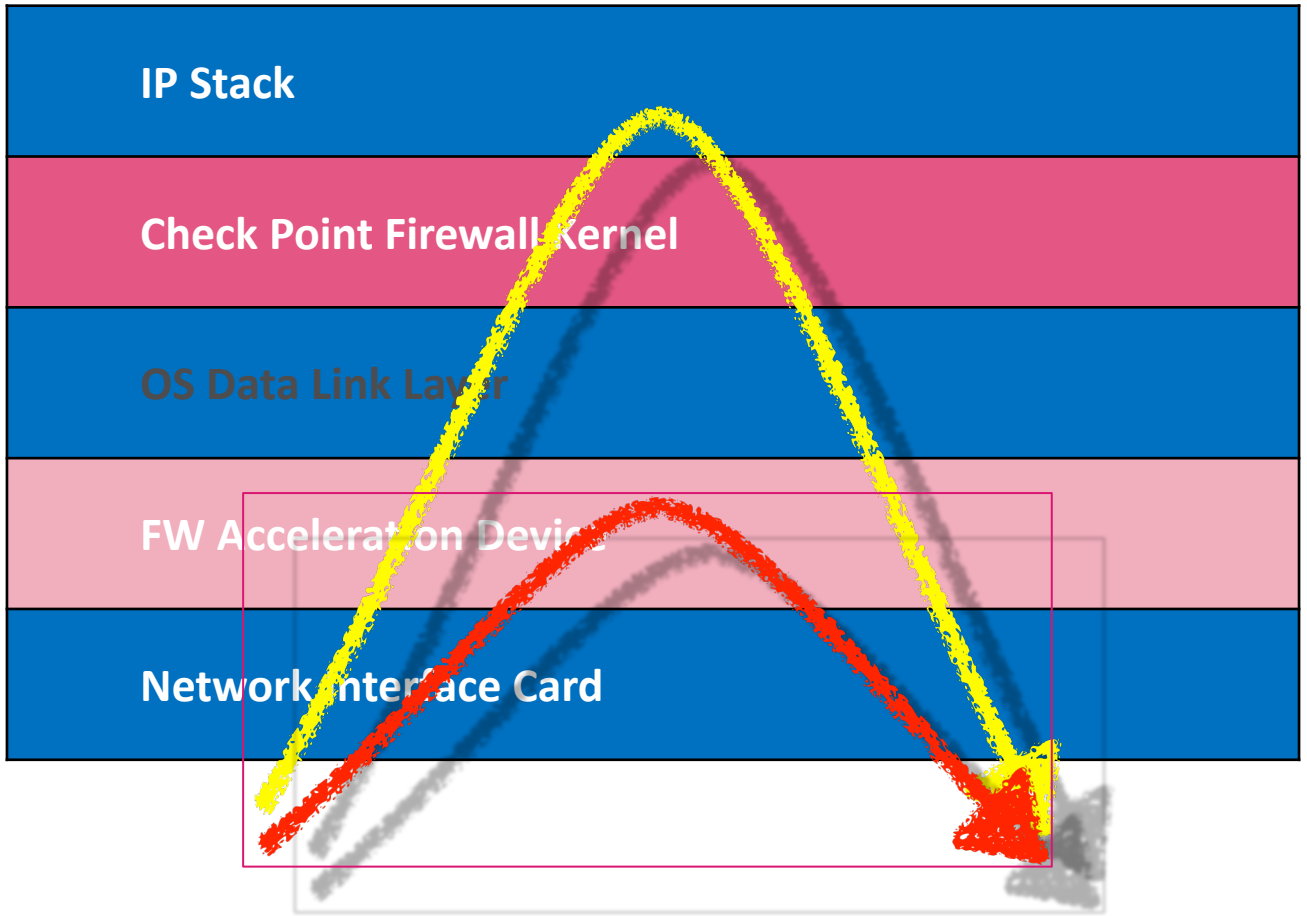
Challenge:

- With growing packet rate and amount of connections, a single CPU FW instance is overwhelmed with security tasks

Approach:

- Offloading some of simple security decision to an additional computation unit (CPU on a card, another core, etc)

SecureXL


IP Stack
Check Point Firewall Kernel
OS Data Link Layer
FW Acceleration Device
Network Interface Card

SecureXL

- sk32578
- Conditional FW bypass without compromising security
- Off-load of lesser security decisions to another CPU, with more efficiency than regular FW
- Throughput acceleration – within the same connection
- Acceleration with templates – improves sessions rate

SECUREXL

UNDER THE HOOD

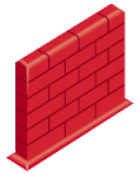
Check Point
CHECKMATES

Two types of acceleration

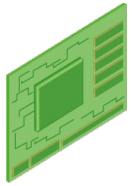
- without templates
- with templates

First packet

Web Server 10.0.0.1



Firewall



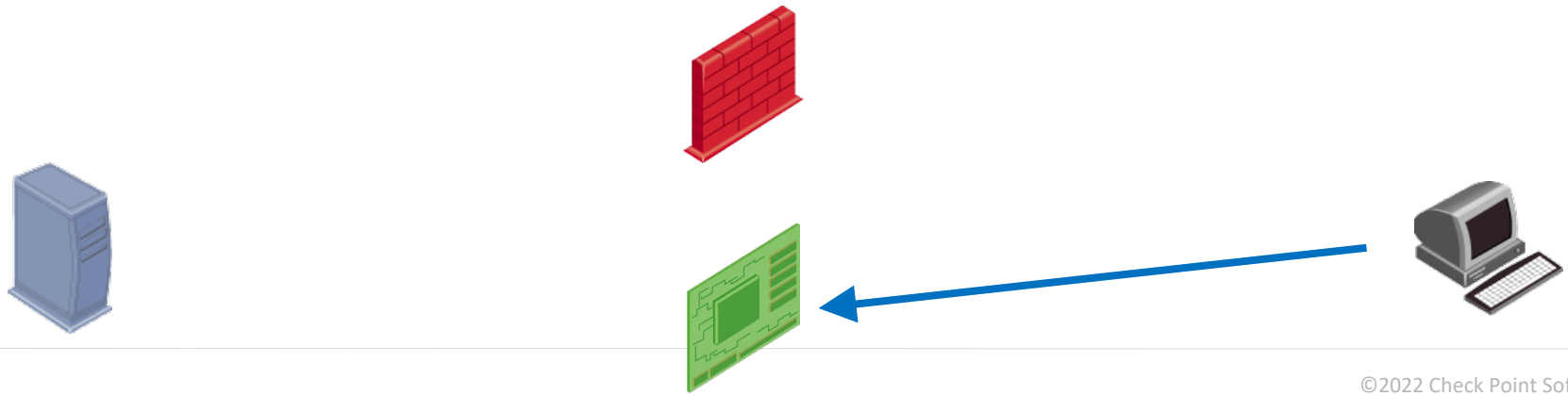
Acceleration Device

Web Client 192.168.0.1

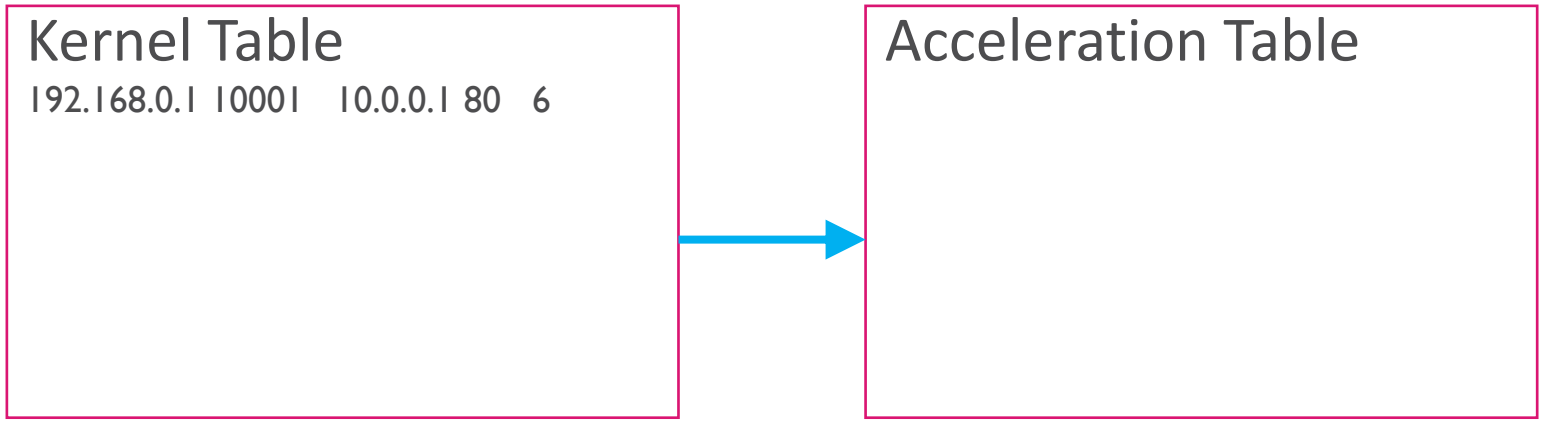
First packet

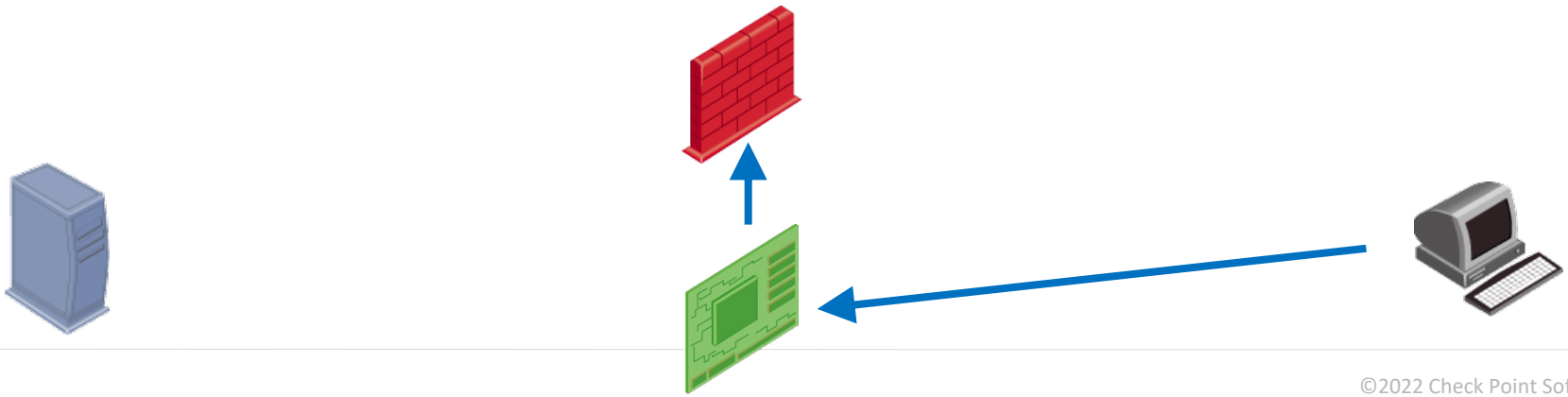
Kernel Table

Acceleration Table

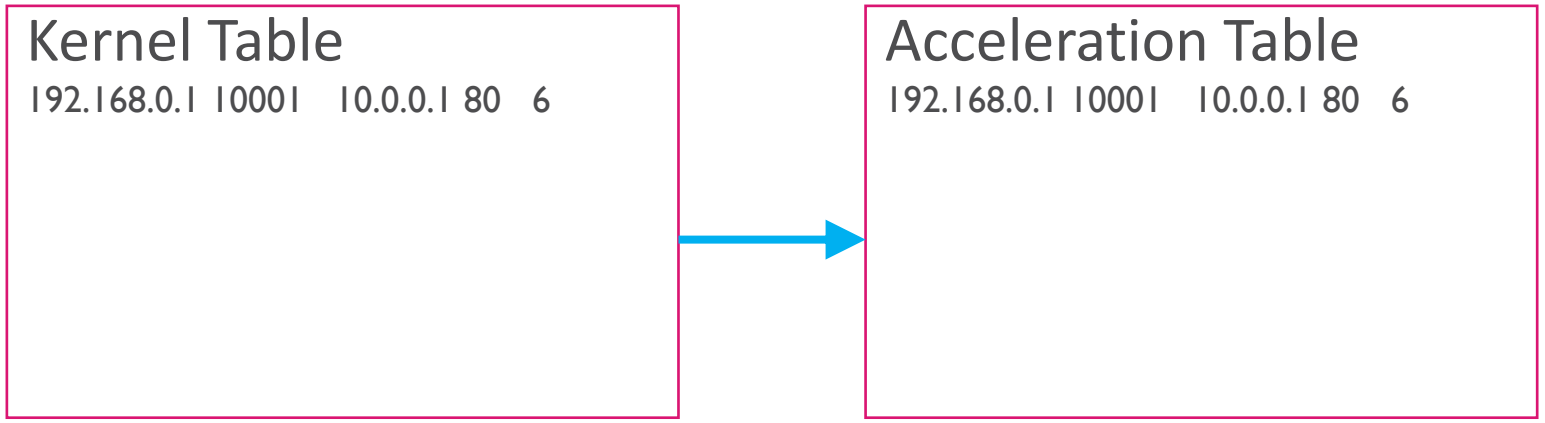


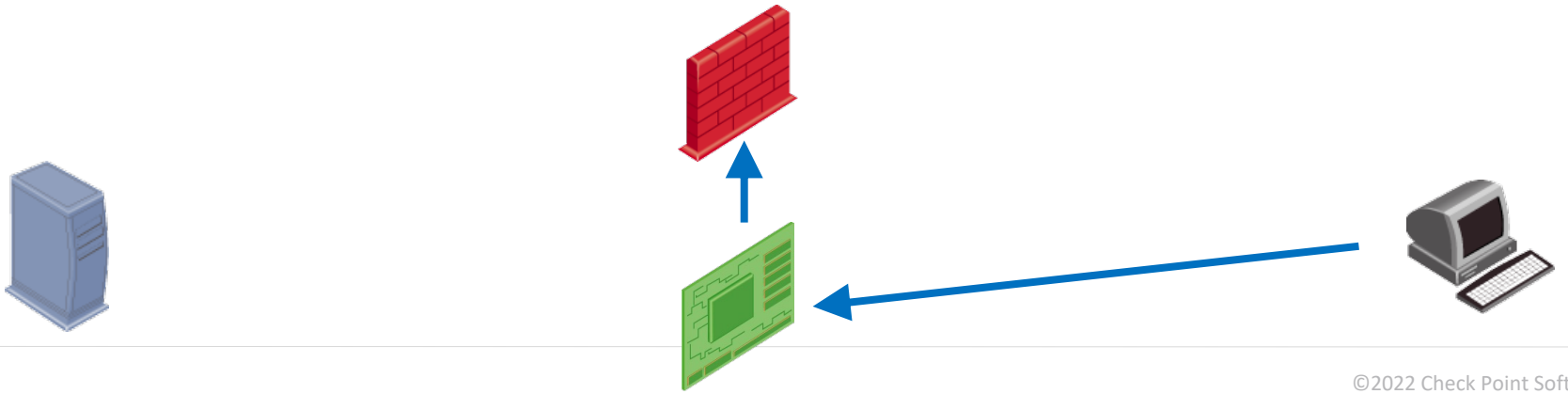
First packet



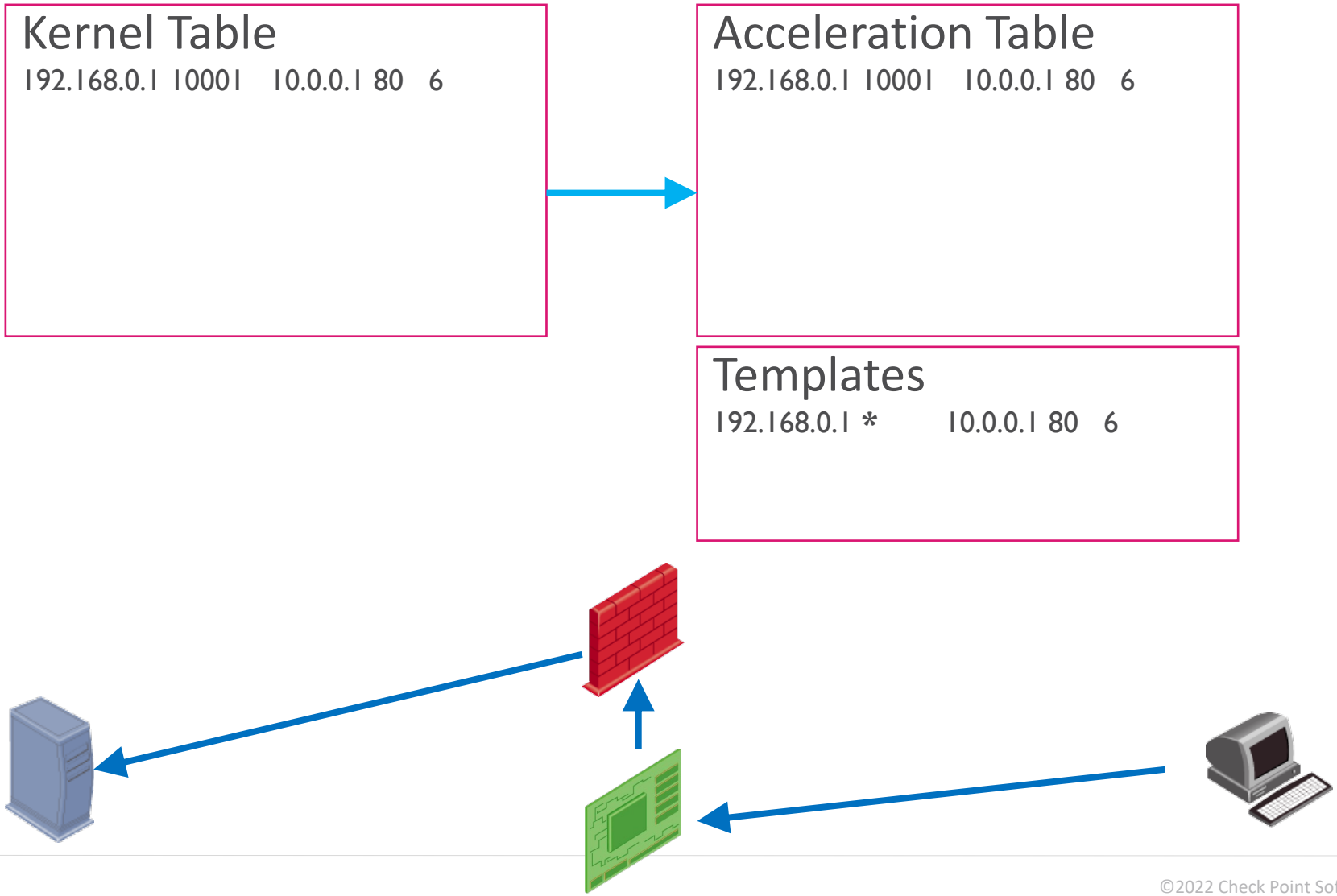


First packet





First packet



Next packets

Kernel Table

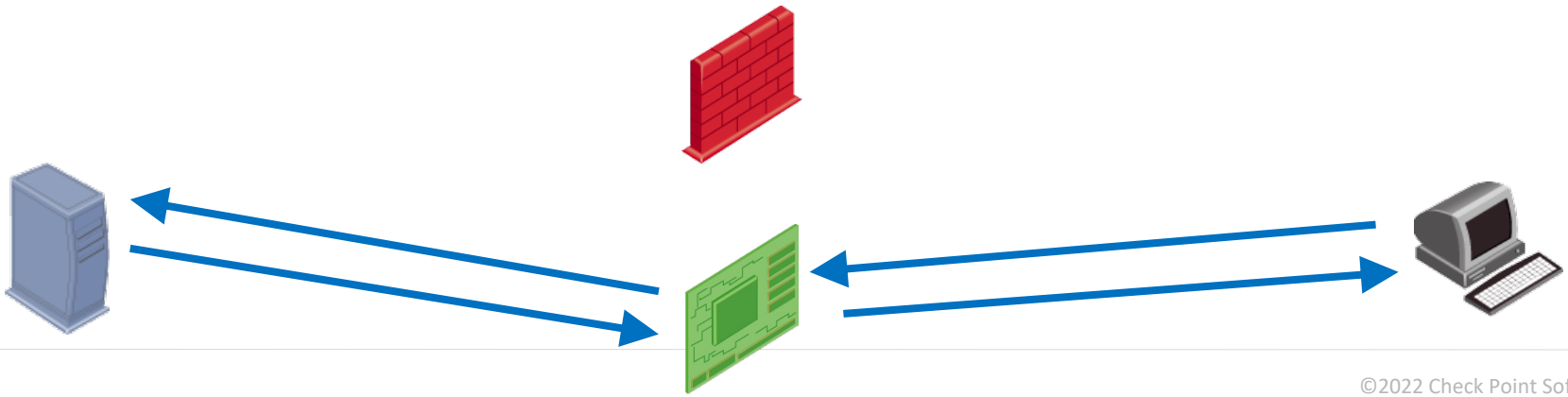
192.168.0.1 10001 10.0.0.1 80 6

Acceleration Table

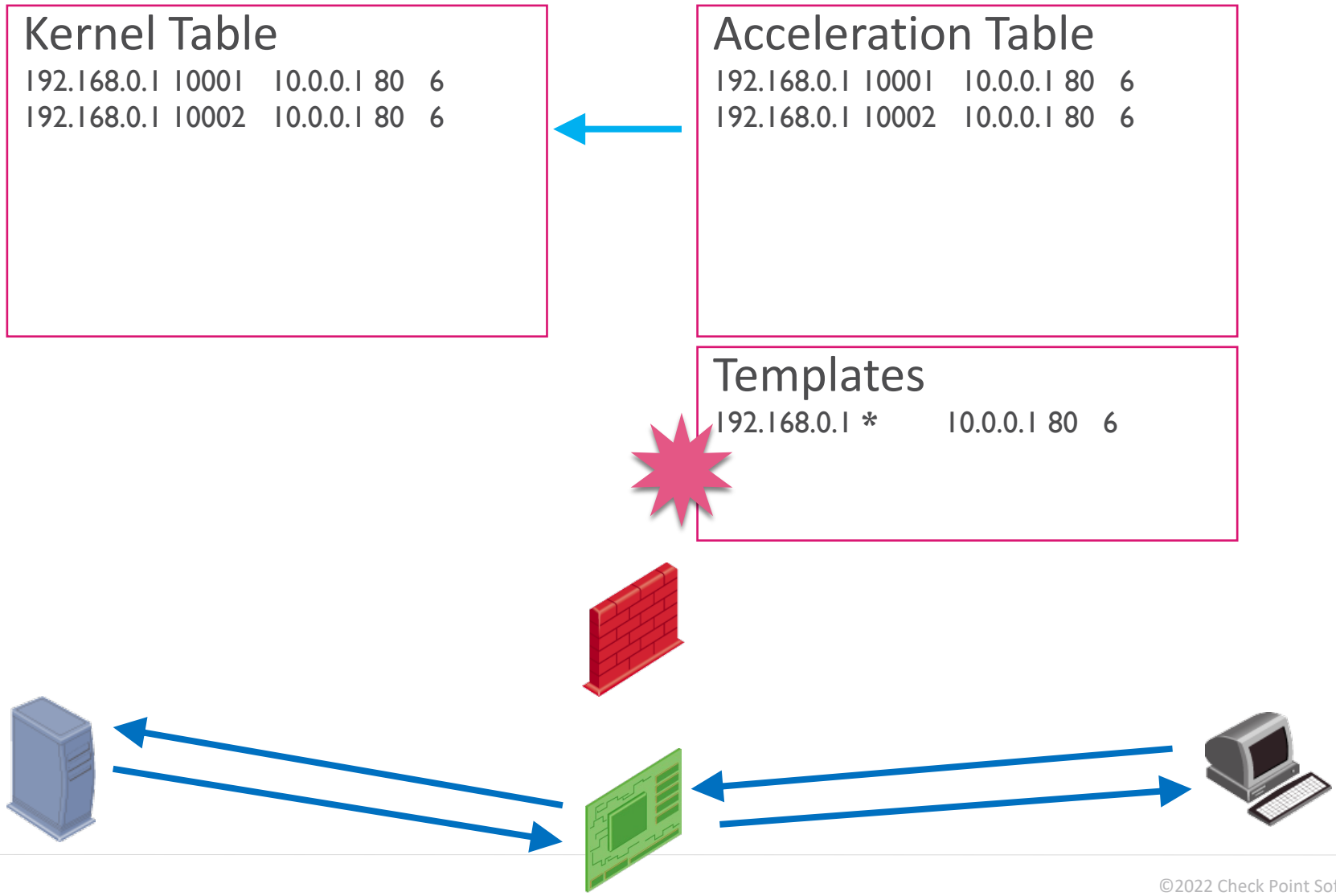
192.168.0.1 10001 10.0.0.1 80 6

Templates

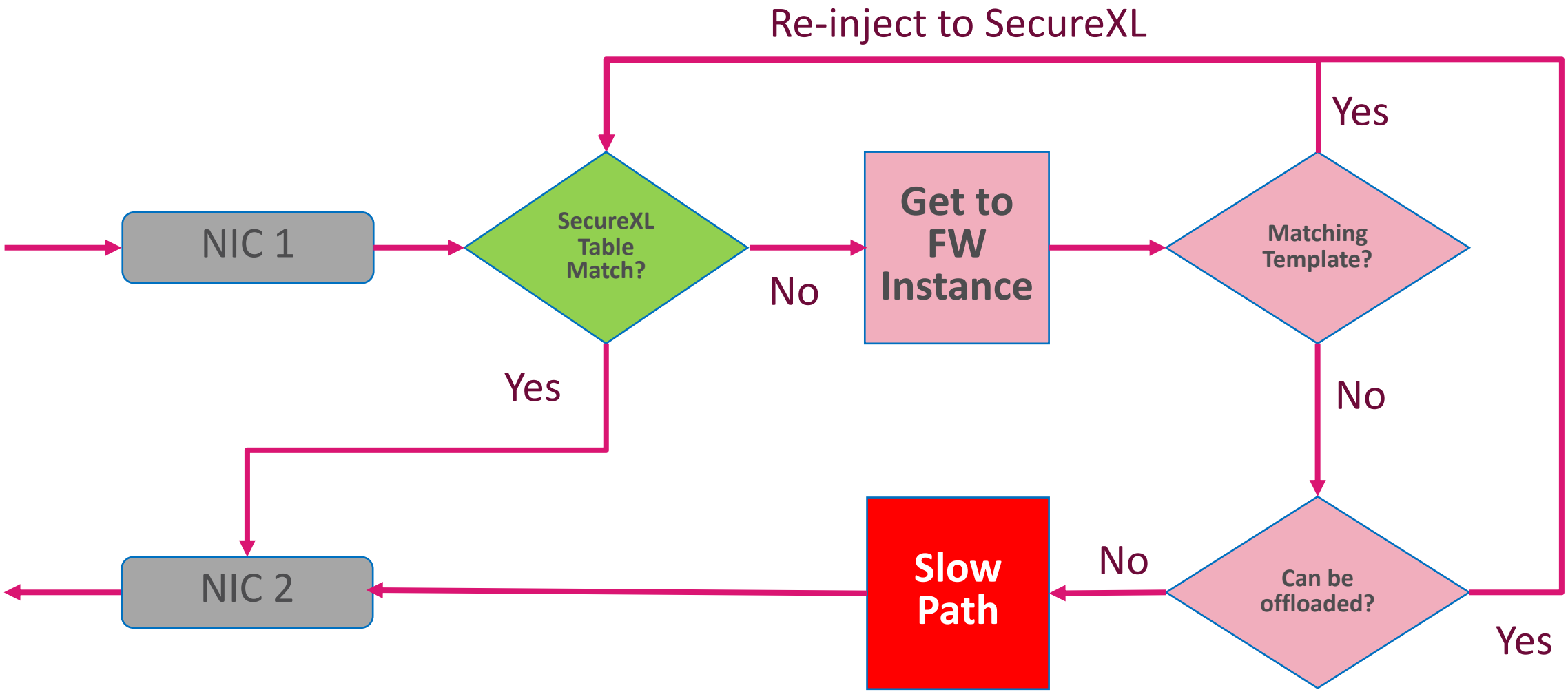
192.168.0.1 * 10.0.0.1 80 6



New connection



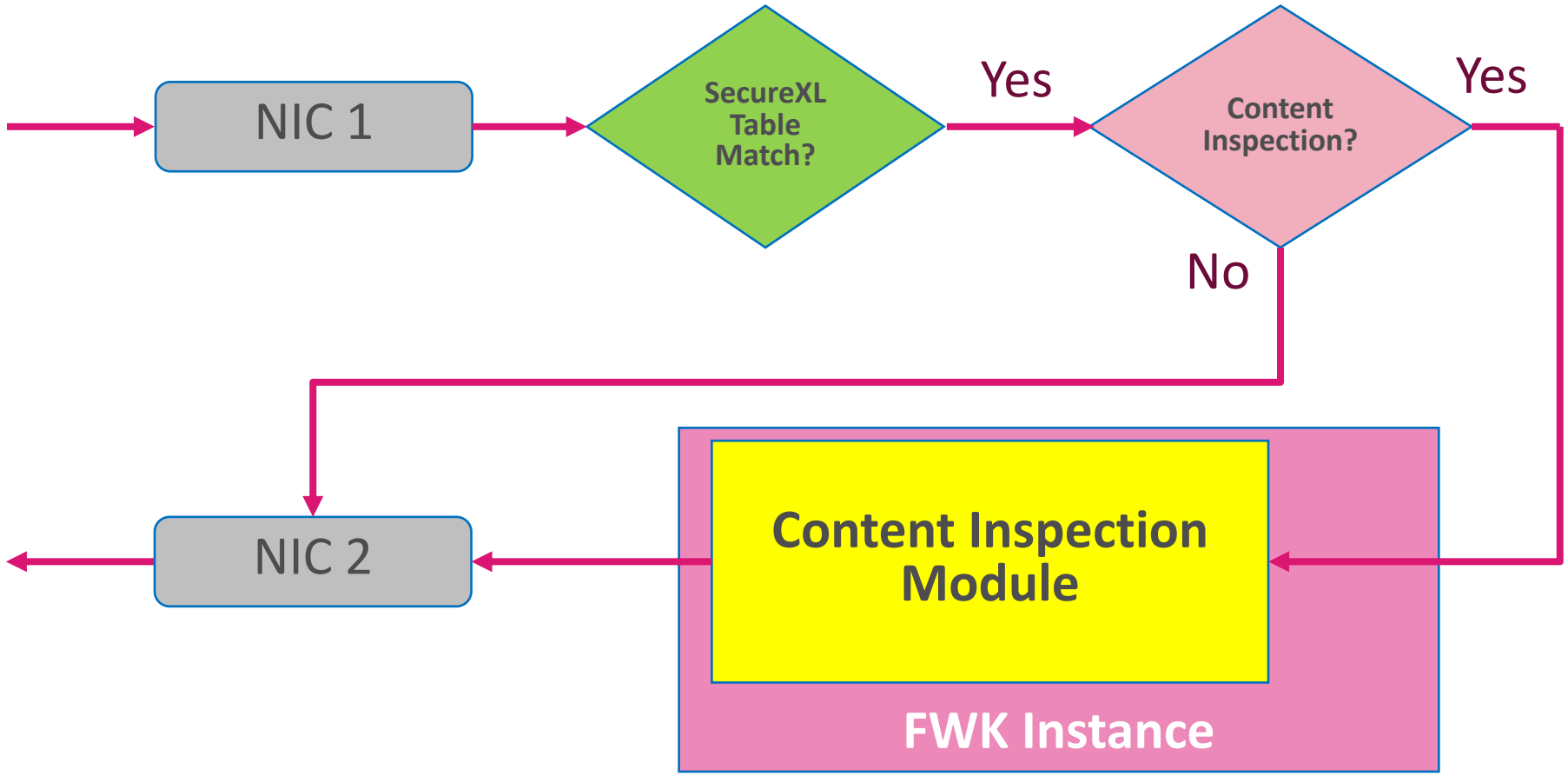
SecureXL – Simplified Flow R80.20 and up sk153832



SecureXL & CoreXL – Paths

- Firewall Path
  - Connection cannot be accelerated
  - All packets within the connections are handled by Firewall Instance
- Accelerated Path
  - All packets are handled by SecureXL
- Medium Path
  - Packet flow is partially handled by SecureXL
  - Data flow is run through Firewall Instances for content inspection
  - Only available with CoreXL

Medium Path R80.20 and up (Simplified)



Special Case - SecureXL Fast Accelerator

- SecureXL Fast Accelerator (fw ctl fast_accel) sk156672
  - Deep packet inspection bypass for trusted assets
  - R80.40
  - R80.30 Take 107
  - R80.20 Take 103
- Bypass deep packet inspection for trusted
- Fast Pass instead of Medium Pass
- Note limit of 10 fast_accel rules (can be increased)

SecureXL Fast Accelerator - controls

```
fw ctl fast_accel <option>
```

- add — Add a connection
- delete — Delete a connection
- enable — Set feature state to on
- disable — Set feature state to off
- show_table — Display the rules configured by the user
- show_state — Display the current feature state
- reset_stats — Reset the statistics collected by the feature
- --help/-h — Display help message

- `fw ctl fast_accel add 1.1.1.1 2.2.2.0/24 80 6`
- `fw ctl fast_accel delete 1.1.1.1 2.2.2.0/24 80 6`

Acceleration Status

```
[Expert@cpmodule]# fwaccel stat
Accelerator Status : on
Templates : enabled

Accelerator Features : Accounting, NAT, Cryptography, Routing,
                       HasClock, Templates, Synchronous,IdleDetection,
                       Sequencing, TcpStateDetect, AutoExpire,
                       DelayedNotif, TcpStateDetectV2, CPLS, WireMode

Cryptography Features : Tunnel, UDPEncapsulation, MD5, SHA1, NULL,
                        3DES, DES, CAST, CAST-40, AES-128, AES-256,
                        ESP, LinkSelection, DynamicVPN, NatTraversal,
                        EncRouting
```

Info offloaded

- NAT parameters
- Encryption (Cryptography) parameters
- Wire Mode on the connection
- Accounting
- Sequence change (SYN defender, SYN Attack)
- Sequence Verifier validations
- Anti-Spoofing Parameters

Offload notes

- The acceleration device will perform these functionalities **without need of FW**
- If FW will receive a packet within an accelerated connection, it will see this packet after NAT or Decryption

fw monitor & tcpdump*

- In older versions, fw monitor only “sees” packets passing FW, not acceleration device,
- tcpdump also cannot show accelerated packets on FW itself

*Before R80.20

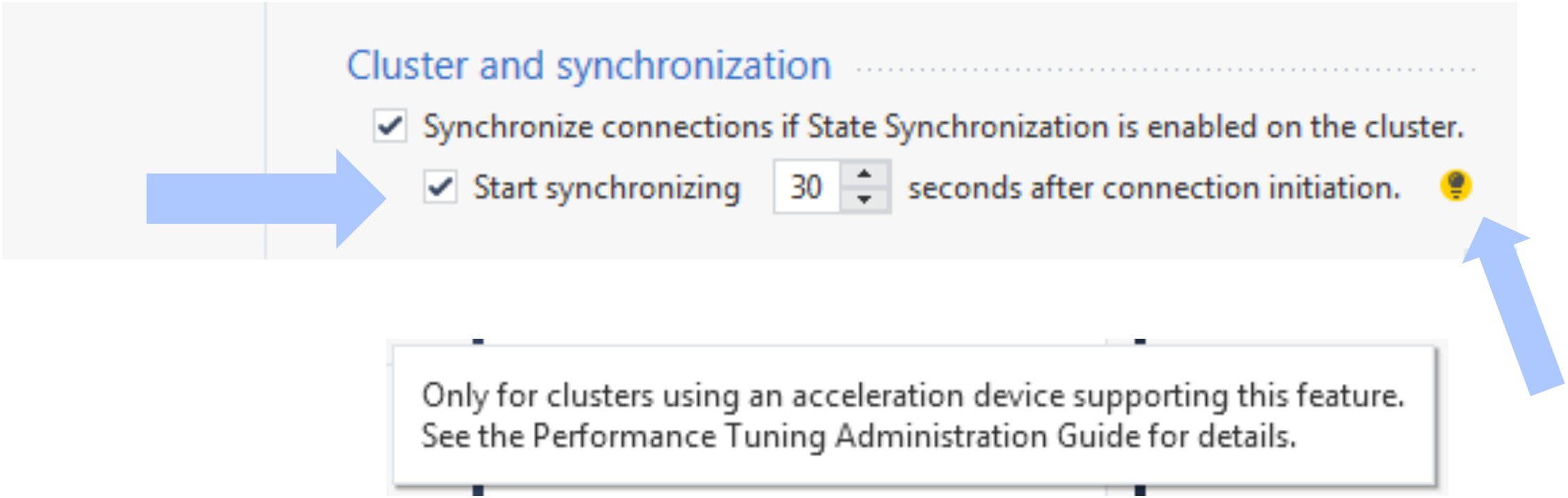
DELAYED NOTIFICATIONS

Check Point
CHECKMATES

Delayed Synchronization in Cluster Environments

- In a cluster setup, services would have to be specifically configured to be delay synchronized.
- The SecureXL connection table is NOT synchronized between cluster members.
- If a connection is created from template, the firewall is unaware of it and thus, the connection is also not synchronized to the standby member.
- Only once the “Delayed Synchronization” timeout has reached (and only in case the connection is still open) the connection will be synchronized to the standby cluster member.

Configuration



SECUREXL LIMITATIONS

Check Point
CHECKMATES

What is not Accelerated?

- First packet in the session
  - Unless TCP session matches acceleration template
- Service with Resource
- Matching rules
  - with drop (unless Drop Optimization is enabled)
  - with reject
  - Where Security Gateway is Source or Destination
  - With User/Session Authentication
- IPv6 Multicast

What is not Accelerated?

- VPN
  - Visitor mode
  - Transport Mode
  - Multicast traffic through VPN tunnel
- Mobile Access Blade
- PPP, PPTP, PPPoE*
- Some connections related to ISP Redundancy (sk104679 for more details)

*PPPoE acceleration is available with Gaia Embedded (SMB)
*In versions prior to R80.20, PPPoE disables SecureXL entirely

Limitations for Templates

- Service with Resource
- Service with a handler
- NAT (Without NAT templates)
- VPN traffic
- Complex connections (FTP, H323, SQL, etc.)
- Rules with legacy Authentication
- RPC/DCOM/DCE-RPC
- Some “older” IPS features (Syn Attack, Small PMTU, Network Quota, etc)

Mind the limitations

```
[Expert@FW]# fwaccel stat
+-------------------------------------------------------------------------------+
|Id|Name      |Status     |Interfaces                |Features                   |
+-------------------------------------------------------------------------------+
|0 |SND       |disabled   |eth4,eth5,eth6,eth7       |Acceleration,Cryptography  |
|  |          |           |                          |Crypto: Tunnel,UDPEncap,MD5,  |
|  |          |           |                          |SHA1,NULL,3DES,DES,AES-128,   |
|  |          |           |                          |AES-256,ESP,LinkSelection,    |
|  |          |           |                          |DynamicVPN,NatTraversal,      |
|  |          |           |                          |AES-XCBC,SHA256               |
+-------------------------------------------------------------------------------+
Accept Templates : disabled by Firewall
                   Layer Network disables template offloads from rule #22
                   Throughput acceleration still enabled.
Drop Templates   : enabled
NAT Templates    : disabled by Firewall
                   Layer Network disables template offloads from rule #22
                   Throughput acceleration still enabled.
```

Very bad for acceleration

No acceleration with

- TTL Fingerprint Scrambling
- IPID Fingerprint Scrambling

Completely disables SecureXL (on R77 and below)

- ClusterXL in a Load Sharing mode with Sticky Decision Function*

* Not relevant for ClusterXL Load Sharing mode in R80.20 and higher (sk162637)

NAT TEMPLATES

Check Point
CHECKMATES

NAT Templates

Sk71200 – up to R80.10

- Disabled by default on R80.10 and below
- Critical for high session rate
- Cover bot Static NAT and Hide NAT
- Require template offload by Firewall

- R80.20 and above - enabled by, done by Firewall

NAT Templates – Manual Control

```
Expert@FW]# fwaccel stat

Accelerator Status : on
Accept Templates : enabled
Drop Templates : disabled
NAT Templates : disabled
```

NAT Templates – Manual Control

```
Expert@FW]# fwaccel stat

Accelerator Status : on
Accept Templates : enabled
Drop Templates : disabled
NAT Templates : enabled
```

Mind the limitations

```
[Expert@FW]# fwaccel stat
+-------------------------------------------------------------------------------+
|Id|Name      |Status     |Interfaces                |Features                   |
+-------------------------------------------------------------------------------+
|0 |SND       |disabled   |eth4,eth5,eth6,eth7       |Acceleration,Cryptography  |
|  |          |           |                          |Crypto: Tunnel,UDPEncap,MD5,  |
|  |          |           |                          |SHA1,NULL,3DES,DES,AES-128,   |
|  |          |           |                          |AES-256,ESP,LinkSelection,    |
|  |          |           |                          |DynamicVPN,NatTraversal,      |
|  |          |           |                          |AES-XCBC,SHA256               |
+-------------------------------------------------------------------------------+
Accept Templates : disabled by Firewall
                   Layer Network disables template offloads from rule #22
                   Throughput acceleration still enabled.
Drop Templates   : enabled
NAT Templates    : disabled by Firewall
                   Layer Network disables template offloads from rule #22
                   Throughput acceleration still enabled.
```

NAT Templates – Manual Control (R80.10 and below)

```
[Expert@FW]# vi $FWDIR/boot/modules/fwkern.conf
cphwd_nat_templates_support=1
cphwd_nat_templates_enabled=1
```

- Set on each FW
- Reboot to activate

OPTIMIZED DROPS

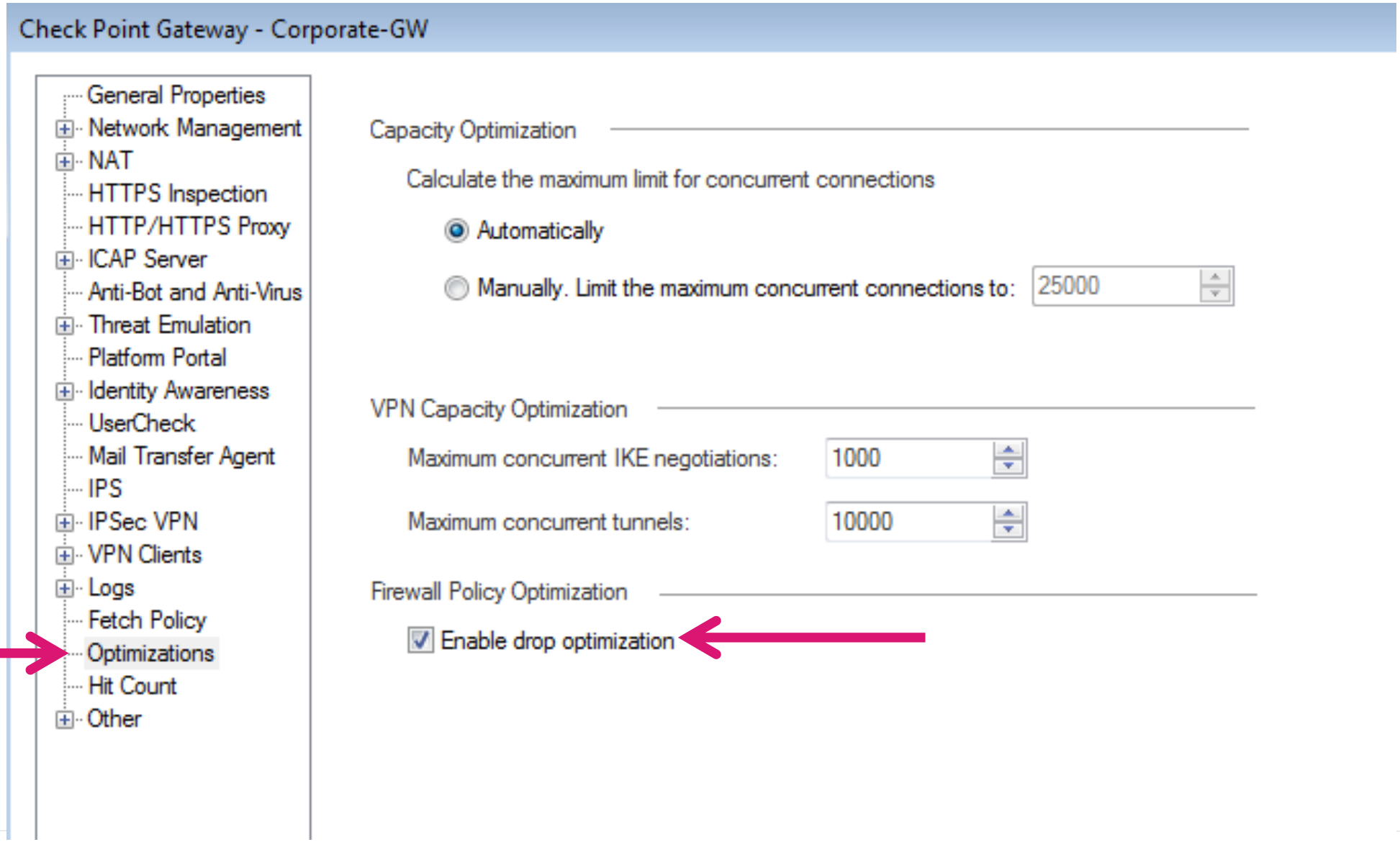
Check Point
CHECKMATES

Drops are bad for performance

- Drop action is done by FW (by default)
- Drop is the heaviest action
- Drop decision is done per packet, not per connection
- It requires rulebase match

- Hence Drop Optimization Feature sk90861 & sk90941

Enabling Optimized Drops



Status

```
[Expert@FW]# fwaccel stat

Accelerator Status : on
Accept Templates : enabled
Drop Templates : enabled
NAT Templates : enabled
```

- or

```
# fw ctl get int fwkern_optimize_drops_support
```

Parameters

- Drop template timeout (default 60 sec)

```
# fw ctl get int cphwd_drop_tmpl_tmo
```

- Dynamic Activation Thresholds
  - optimize_drops_absolute_threshold (default 100)
  - optimize_drops_activation_threshold (default 6)
  - optimize_drops_deactivation_threshold (default 2)

- Plus average drop rate (packets per second)

Logic

- optimize_drops_absolute_threshold=**X**
- optimize_drops_activation_threshold=**Y**
- optimize_drops_deactivation_threshold=**Z**

- Let’s assume that average drop rate is **N** packets per second

Logic - Activation

if

[*average number of drops/sec during the last 30 sec*] > [***X***]

and

[*average number of drops/sec during the last 30 sec*] >= [*(**Y**) x (**N**)*]

then

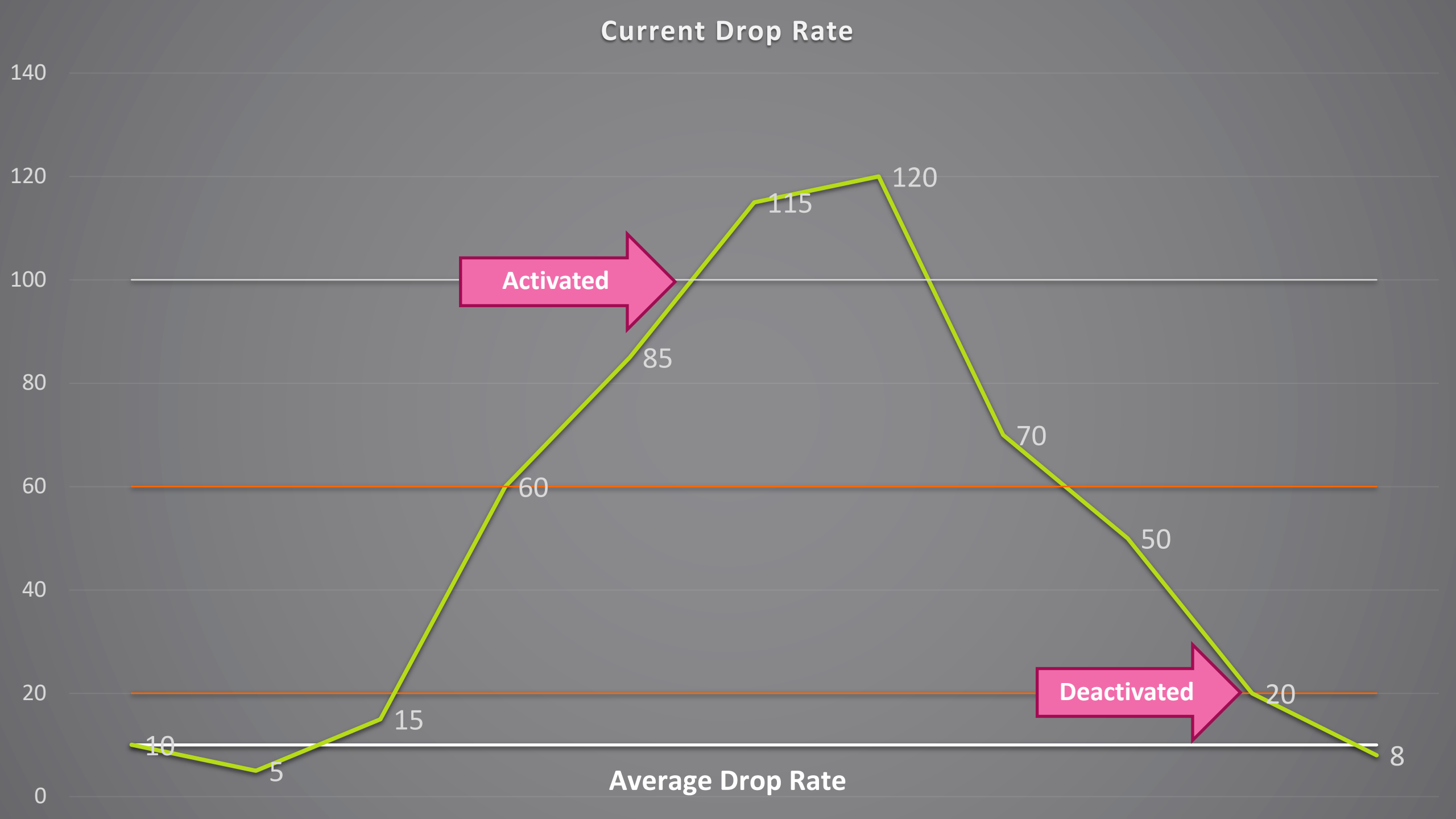
activate the Optimized Drops feature

Logic – Deactivation

if

[average number of drops/sec during the last 30 sec] <= [*(**Z**) x (**N**)*] **then**

deactivate the Optimized Drops feature


Current Drop Rate
140
120
100
80
60
40
20
0
Activated
Deactivated
10
5
15
60
85
115
120
70
50
20
8
Average Drop Rate

DOS MITIGATION

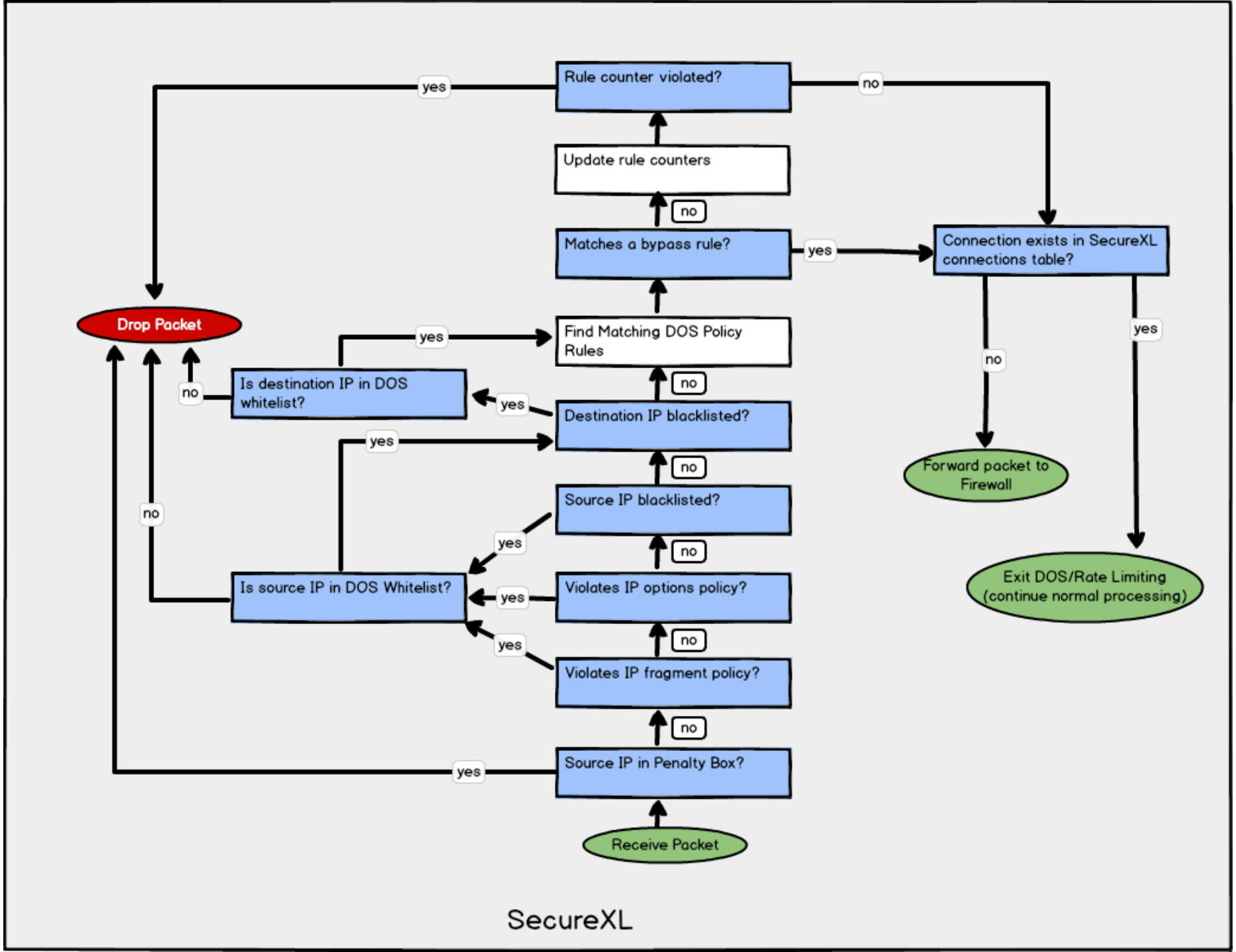
Check Point
CHECKMATES

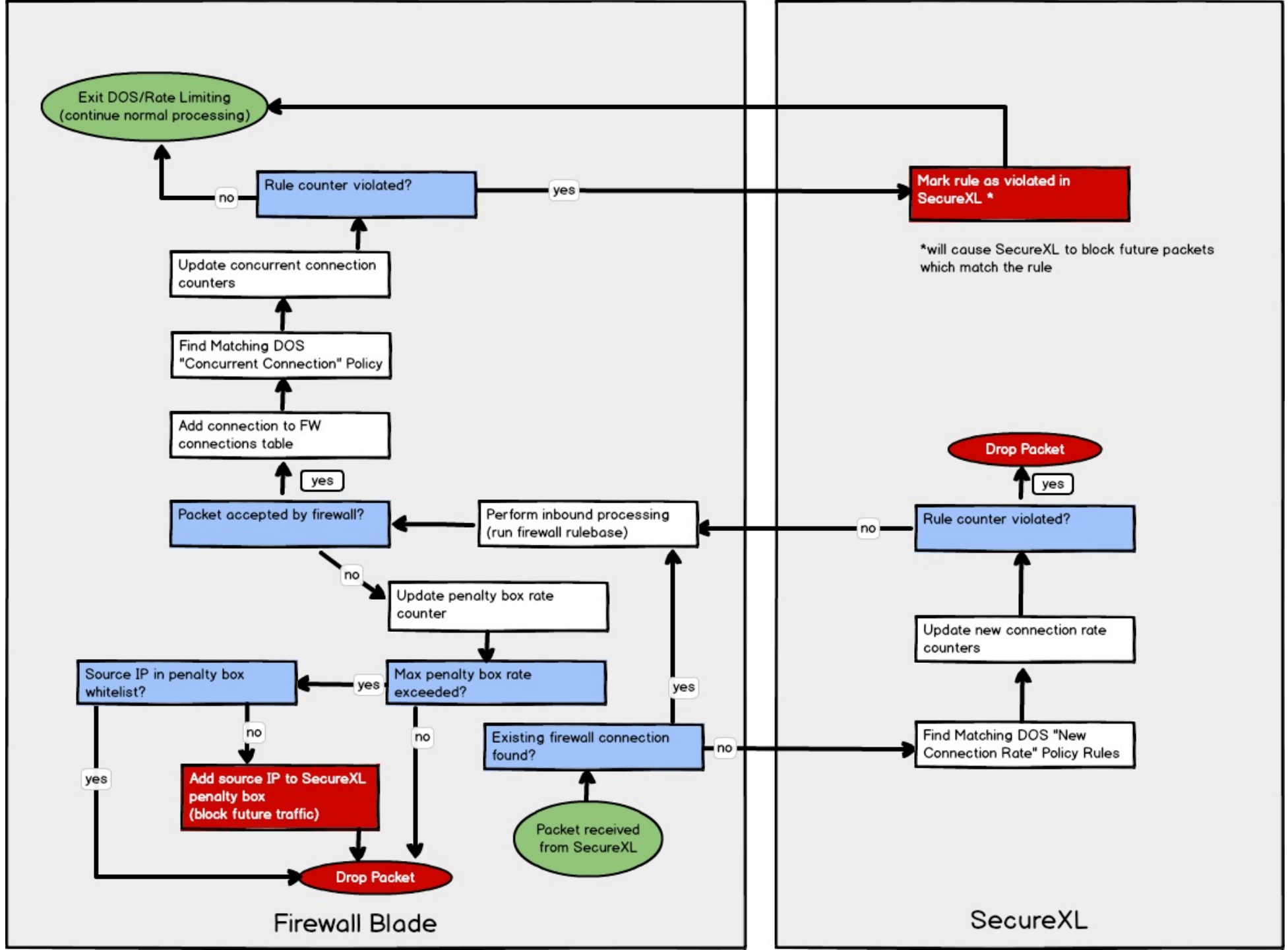
Rate Limiting rules for DoS Mitigation

- Defense against DoS (Denial of Service) attacks
- Limiting traffic
  - coming from specific sources
  - sent to specific destination
  - and using specific services.
- Rate limiting is enforced by SecureXL based on:
  - Bandwidth and packet rate
  - Number of concurrent connections
  - Connection rate

Rate Limiting rules for DoS Mitigation

- R80.20 and up sk112454
  - Incorporates Penalty Box feature (R80.10 and below) sk74520
- Includes the following features:
  - Policy Rules
  - IP Block List
  - Block IP Fragments
  - Block IP Options
  - Penalty Box
  - DoS Allow List
  - Penalty Box Allow List


Rule counter violated?
yes
no
Update rule counters
no
Matches a bypass rule?
yes
Connection exists in SecureXL connections table?
Drop Packet
Find Matching DOS Policy Rules
yes
no
Is destination IP in DOS whitelist?
no
yes
Destination IP blacklisted?
yes
no
Source IP blacklisted?
no
yes
Is source IP in DOS Whitelist?
Violates IP options policy?
yes
no
yes
Violates IP fragment policy?
no
Source IP in Penalty Box?
yes
Receive Packet
Forward packet to Firewall
Exit DOS/Rate Limiting (continue normal processing)
SecureXL


Exit DOS/Rate Limiting
(continue normal processing)
Rule counter violated?
no
yes
Mark rule as violated in SecureXL *
*will cause SecureXL to block future packets which match the rule
Update concurrent connection counters
Find Matching DOS "Concurrent Connection" Policy
Add connection to FW connections table
yes
Drop Packet
yes
Packet accepted by firewall?
Perform inbound processing (run firewall rulebase)
no
Rule counter violated?
no
Update penalty box rate counter
Update new connection rate counters
Source IP in penalty box whitelist?
yes
Max penalty box rate exceeded?
yes
yes
no
no
Existing firewall connection found?
no
Find Matching DOS "New Connection Rate" Policy Rules
Add source IP to SecureXL penalty box (block future traffic)
Packet received from SecureXL
Drop Packet
Firewall Blade
SecureXL

TRAFFIC VISIBILITY CHALLENGE

Check Point
CHECKMATES

fw monitor – R80.20 and up (sk30583)

- Since R80.20, 1st Accelerated packet will be monitored only in inbound (i)
- Since R80.20 Jumbo take 73, Accelerated traffic in fast path will monitor inbound and outbound
- Since R80.20 Jumbo take 117, Slow Path, Med Path and Fast Path are monitored
- In R80.30, default behavior is like R80.20 prior to Jumbo take 72
- In R80.40, Default behavior will be to monitor all traffic

Cannot see accelerated traffic

- `fw monitor` may only see info for packets crossing FW kernel modules
  - depending on version, see sk30583 for more details
- `tcpdump` also cannot show accelerated packets either

- What to do?
  - Use cppcap
  - Disable acceleration
  - …But sometimes it does not work

I cannot disable acceleration!

R80.20 and above - sk162492

- SecureXL is off, but traffic is still accelerated. Why?
  - Communication between SecureXL and Firewall-1 is now asynchronous
  - All connections that were accelerated will continue to be handled by Performance Pack
- What to do?
  - Disable acceleration on both cluster members
  - Fail over
  - Run traces on the new active member

Disable SecureXL for specific IP Addresses - sk104468

$FWDIR/lib/table.def on your management

```
/*
 * The following tables force TCP and UDP connections to be
 * forwarded to the firewall according to their tuples.
 *
 * src          Source IP address
 * dst          Destination IP address
 * dport        Destination port
 */
/* tcp_f2f_ports = { <dport> }; */
/* udp_f2f_ports = { <dport> }; */
/* tcp_f2f_conns = { <src, dest, dport> }; */
/* udp_f2f_conns = { <src, dest, dport> }; */
```

Disable SecureXL for specific IP Addresses - sk104468

$FWDIR/lib/table.def on your management

- Backup the table first!
- Add new entry:

```
f2f_addresses =
{
<IP_ADDRESS_1> ,
<IP_ADDRESS_2> ,
<IP_ADDRESS_3>
};
```

- Range example

```
f2f_addresses = {<10.0.0.0, 10.0.0.255>, <192.168.0.0,
192.168.0.255>};
```

Disable SecureXL for specific IP Addresses - sk104468

- **Caution:**
  This is a global table! Install policy **only** on FW/Cluster you investigate!
- Upon policy installation:

```
# fw tab -t f2f_addresses
```

- Check the required addresses are listed

- When finished, revert back the file and push policy again

OTHER ACCELERATION TECHNOLOGIES

Check Point
CHECKMATES

Announced on CPX and discussed on CheckMates

- **LightSpeed Appliances**
  with NVIDIA 2-port 100G cards - sk176466

- **Quantum HyperFlow**
  New solution for Heavy Connections, available in R81.20

SECUREXL DIAGNOSTICS BASICS

Check Point
CHECKMATES

SecureXL diagnostics

- **cpview**
  - SecureXL status and statistics
- **fwaccel stat**

```
Accelerator Status : on
Accept Templates   : disabled by Firewall
                              disabled from rule #31
Drop Templates     : disabled
NAT Templates      : disabled by user

Accelerator Features : Accounting, NAT, Cryptography, Routing,
                       HasClock, Templates, Synchronous, IdleDetection,
                       Sequencing, TcpStateDetect, AutoExpire,
                       DelayedNotif, TcpStateDetectV2, CPLS, WireMode,
                       DropTemplates, NatTemplates, Streaming,
                       MultiFW, AntiSpoofing, ViolationStats,
                       Nac, AsychronicNotif, ERDOS
Cryptography Features : Tunnel, UDPEncapsulation, MD5, SHA1, NULL,
                        3DES, DES, CAST, CAST-40, AES-128, AES-256,
                        ESP, LinkSelection, DynamicVPN, NatTraversal,
                        EncRouting, AES-XCBC, SHA256
```

SecureXL diagnostics, cont.

- **fwaccel stats -s**
  - summary of SecureXL acceleration statistics

```
Accelerated conns/Total conns : 364/13215 (2%)
Delayed conns/(Accelerated conns + PXL conns) : 48/12023 (0%)
Accelerated pkts/Total pkts   : 18252/564927 (3%)
F2Fed pkts/Total pkts   : 36776/564927 (6%)
PXL pkts/Total pkts   : 509899/564927 (90%)
QXL pkts/Total pkts   : 0/564927 (0%)
```

SecureXL diagnostics, cont.

- `fwaccel stats`

```
Medium Streaming Path
-------------------------------------------------------------------------------
CPASXL packets                          0    PSLXL packets                      0
CPASXL async packets                    0    PSLXL async packets                0
CPASXL bytes                            0    PSLXL bytes                        0
C CPASXL conns                          0    C PSLXL conns                      0
CPASXL conns created                    0    PSLXL conns created                0
PXL FF conns                            0    PXL FF packets                     0
PXL FF bytes                            0    PXL FF acks                        0
PXL no conn drops                       0
```

- Look at FF numbers
  - NGFW may result in a high FF rate.

SecureXL diagnostics, cont.

- **fwaccel conns**
  - Displays entries from SecureXL connections table

```
Source          SPort Destination     DPort PR Flags   C2S i/f   S2C i/f
--------------- ----- --------------- ----- -- ------- --------- ---------
   X.X.X.X      61242    X.X.X.X        80  6 ..N.... eth5/eth0 eth0/eth5
   X.X.X.X       6000    X.X.X.X      3842  6 ....... eth0/eth4 eth4/eth0
   X.X.X.X       1620    X.X.X.X        88 17 ....... eth4/eth2 eth2/eth4
   X.X.X.X      50829    X.X.X.X        80  6 ..N.... eth5/eth0 eth0/eth5
   X.X.X.X       4285    X.X.X.X        80  6 F.N.... eth5/eth0 eth0/eth5
   X.X.X.X         80    X.X.X.X     49312  6 F.N.... eth5/eth0 eth0/eth5
   X.X.X.X         80    X.X.X.X     11450  6 ..N.... eth5/eth0 eth0/eth5
   X.X.X.X      58562    X.X.X.X        80  6 F.N.... eth5/eth0 eth0/eth5
   X.X.X.X        161    X.X.X.X      5002 17 F...... eth2/eth2 -/-
   X.X.X.X      21891    X.X.X.X         0  1 F...... eth2/eth4 eth4/eth2
   X.X.X.X      34303    X.X.X.X       389  6 F.N.... eth2/eth2 eth2/-
```

SecureXL diagnostics, cont.

- **fwaccel templates**
  - Displays SecureXL Connection Templates

```
Source          SPort Destination   DPort PR  Flags      LCT DLY C2S i/f S2C i/f Inst Identity
-------------- ----- ------------ ----- -- --------- ---- --- ------- ------- ---- --------
  X.X.X.X       *     X.X.X.X        161 17 ...A...S.   65   0 36/21   21/36    0        0
  X.X.X.X       *     X.X.X.X        161 17 ...A...S.    5   0 36/8    8/36     1        0
  X.X.X.X       *     X.X.X.X       1437 17 ...A...S.   27   0 36/8    8/36     1        0
  X.X.X.X       *     X.X.X.X        161 17 ...A...S.   23   0 36/21   21/36    2        0
  X.X.X.X       *     X.X.X.X         88 17 ...A...S.   11   0 8/36    36/8     4        0
```

- **sim if / fwaccel if**
  - Displays the list of interfaces used and seen by the SecureXL

```
Name       | Address          | MTU   | F   | SIM F | IRQ | Dev         | Output
-----------------------------------------------------------------------------
eth0       | 172.30.168.38    | 1500  | 039 | 00000 |  67 | 0x85b1b000  | 0xffffffff
eth1       | 10.20.30.38      | 1500  | 029 | 00008 |  75 | 0xbc5d3000  | 0xffffffff
eth2       | 10.5.0.1         | 1500  | 029 | 00000 |  83 | 0xbcbbb000  | 0xffffffff
```

SecureXL diagnostics, cont.

- **sim affinity -l***
  - Displays the current affinity of network interfaces to CPU cores

```
eth0 : 0
eth1 : 0
eth2 : 1
eth3 : 1
```

***fwaccel affinity** command with **3.10** kernel

SecureXL diagnostics, cont.

- **cat /proc/ppk/conf**
- Displays SecureXL configuration and basic statistics

```
Flags                                 : 0x00009a16
Accounting Update Interval            : 60
Conn Refresh Interval                 : 512
SA Sync Notification Interval         : 0
UDP Encapsulation Port                : 0
Min TCP MSS                           : 0
TCP Auto-Expire Timeout               : 20
Connection Limit                      : 18446744073709551615
TmplQuota Enabled                     : 0
TmplQuota Quota (rate)                : 512
TmplQuota Drop Dduration              : 300
TmplQuota Monitor only                : 0
TmplQuota Dropped pkts                : 0

Total Number of conns                 : 54
Number of F2F conns                   : 54
Number of Crypt conns                 : 0
Number of TCP conns                   : 18
Number of Non-TCP conns               : 36
Number of Delayed TCP conns           : 0
Number of Delayed Non-TCP conns       : 0
```

SecureXL diagnostics, cont.

- **cat /proc/ppk/statistics**
- Displays SecureXL statistics (same as **fwaccel stats -l**)

Name	Value	Name	Value
conns created	67518	conns deleted	67475
temporary conns	0	templates	0
nat conns	0	accel packets	0
accel bytes	0	F2F packets	16599213
ESP enc pkts	0	ESP enc err	0
ESP dec pkts	0	ESP dec err	0
ESP other err	0	espudp enc pkts	0
espudp enc err	0	espudp dec pkts	0
espudp dec err	0	espudp other err	0
AH enc pkts	0	AH enc err	0
AH dec pkts	0	AH dec err	0
AH other err	0	memory used	0
free memory	0	acct update interval	60
current total conns	43	TCP violations	0
conns from templates	0	TCP conns	15
delayed TCP conns	0	non TCP conns	28
delayed nonTCP conns	0	F2F conns	43
F2F bytes	1076600709	crypt conns	0
enc bytes	0	dec bytes	0
partial conns	0	anticipated conns	0
dropped packets	0	dropped bytes	0
nat templates	0	port alloc templates	0
conns from nat templ	0	port alloc conns (tm	0
port alloc f2f	0	PXL templates	0
PXL conns	0	PXL packets	0
PXL bytes	0	PXL async packets	0
conns auto expired	0	C used templates	0
pxl tmpl conns	0	C conns from tmpl	0
C non TCP F2F conns	28	C tcp handshake conn	14
C tcp established co	1	C tcp closed conns	0
C tcp f2f handshake	14	C tcp f2f establishe	1
C tcp f2f closed con	0	C tcp pxl handshake	0
C tcp pxl establishe	0	C tcp pxl closed con	0
QXL templates	0	QXL conns	0
QXL packets	0	QXL bytes	0
QXL async packets	0	outbound packets	0
outbound pxl packets	0	outbound f2f packets	124862
outbound bytes	0	outbound pxl bytes	0
outbound f2f bytes	33552839	trimmed pkts	0

SecureXL diagnostics, cont.

- **cat /proc/ppk/statistics**
- Displays SecureXL drop statistics

Reason	Packets	Reason	Packets
general reason	0	PXL decision	0
fragment error	0	hl - spoof viol	0
F2F not allowed	0	hl - TCP viol	0
corrupted packet	0	hl - new conn	0
clr pkt on vpn	0	partial conn	0
encrypt failed	0	drop template	0
decrypt failed	0	outb - no conn	0
interface down	0	cluster error	0
XMT error	0	template quota	0
anti spoofing	0	Attack mitigation	0
local spoofing	0	sanity error	0
monitored spoofed	0	QXL decision	0

SecureXL diagnostics, cont.

- **cat /proc/ppk/viol_statistics**
- Displays violations statistics

Violation	Packets	Violation	Packets
pkt is a fragment	0	pkt has IP options	406
ICMP miss conn	932	TCP-SYN miss conn	169
TCP-other miss conn	17	UDP miss conn	10305933
other miss conn	0	VPN returned F2F	0
ICMP conn is F2Fed	7	TCP conn is F2Fed	23665
UDP conn is F2Fed	6275273	other conn is F2Fed	0
uni-directional viol	0	possible spoof viol	0
TCP state viol	0	out if not def/accl	0
bridge, src=dst	0	routing decision err	0
sanity checks failed	0	temp conn expired	0
fwd to non-pivot	0	broadcast/multicast	0
cluster message	0	partial conn	0
PXL returned F2F	0	cluster forward	0
chain forwarding	0	general reason	0

SecureXL diagnostics, cont.

- **cat /proc/ppk/mcast_statistics**
- Displays SecureXL multicast statistics

Name	Value	Name	Value
in packets	406	out packets	0
if restricted	0	conns with down if	0
f2f packets	0	f2f bytes	0
dropped packets	0	dropped bytes	0
accel packets	0	accel bytes	0
mcast conns	1		

A WORD ABOUT QUANTUM SPARK (SMB APPLIANCES)

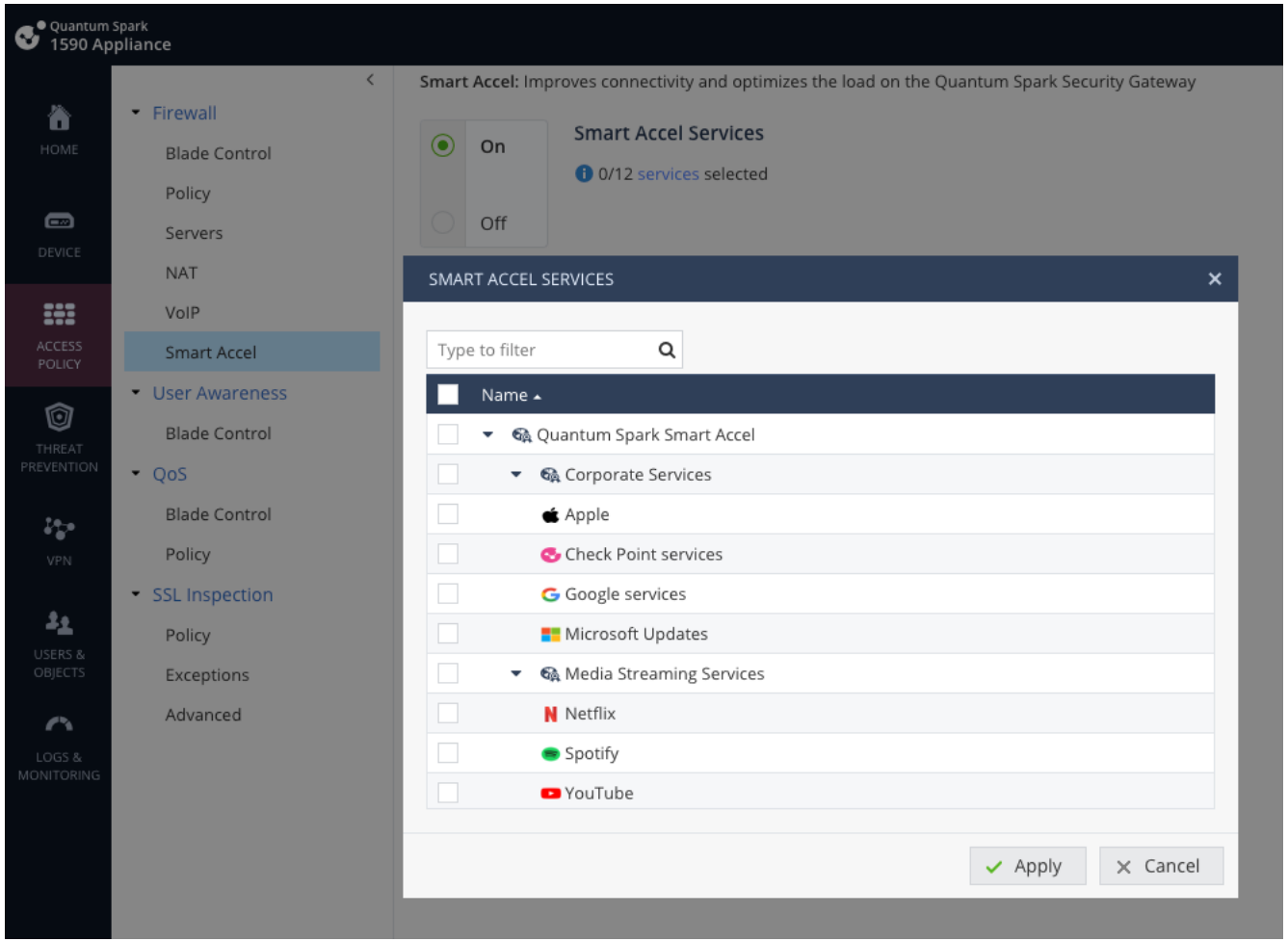
Check Point
CHECKMATES

SecureXL and SMB

- Works exactly the same as on non-SMB gateways
- Most troubleshooting in this presentation also applies to SMB
- A few limitations
  - cpview is not available in R80.20.xx and earlier firmware
  - Disabling SecureXL for specific traffic requires a different process on locally managed SMB appliances (see sk164793)

SmartAccel for Quantum Spark Appliances

- Available in R81.10 firmware
- Allows specific low-risk services/applications to be fully accelerated by SecureXL, improving performance.



Need more?

NEED MORE?

WAIT FOR PART 5 – DIAGNOSTICS HOW TO

Check Point
CHECKMATES

Further reading

- Best Practices - Security Gateway Performance - sk98348
- SecureXL - sk153832 - ATRG: SecureXL for R80.20 and higher
- CoreXL - sk98737 - ATRG: CoreXL
- SMT (HyperThreading) - sk93000 - SMT (HyperThreading) Feature Guide
- Multi-Queue - sk80940
- ClusterXL - sk93306 - ATRG: ClusterXL
- VPN - sk105119 - Best Practices - VPN Performance and to sk104760 - ATRG: VPN Core

QUESTIONS?

Check Point
CHECKMATES

Full list of Performance Series

- Part 1 – Introduction
- **Part 2 – SecureXL**
- Part 3 – CoreXL
- Part 4 – Clustering and Hyperscale
- Special– Diagnostics How To

THANK YOU

Check Point
CHECKMATES